VACANCY

RE-ADVERTISEMENT

REFERENCE NR	**:**	**RE-SM_10_2018**
JOB TITLE	**:**	**Senior Manager: Security Development X1**
JOB LEVEL	**:**	**D5**
SALARY	**:**	**R 612 887 – R 1 021 478**
REPORT TO	**:**	**Head of Department: Information Security Services**
DIVISION	**:**	**Hosting & Secure Operations**
Department	**:**	**Information System Security**
LOCATION	**:**	**SITA Erasmuskloof**
POSITION STATUS	**:**	**Permanent (Internal/External)**

Purpose of the job

To lead and manage the Security Development unit within the Information Security department to develop, implement and maintain solution security architecture and solutions to ensure that government information/data, infrastructure and applications are secured, in accordance with ICT standards and the enterprise architecture for Government. This includes identifying, plan and developing of security measures to safeguard information against accidental or unauthorized modification, destruction or disclosure for data, solutions, hardware, telecommunications and computer installations.

Key Responsibility Areas

Support the Solution Security in developing and implementing Solution Security strategies and roadmaps (from a Security Development perspective) to ensure a comprehensive and integrated Solution Security function; Participate in the development, implementation and evaluation of governance mechanisms for Security Development within Solution Security and monitor the adherence thereto so as to deliver quality products in a controlled environment;

Lead and Manage resources (i.e. budget/finances, asset/equipment and staff) within the Unit in order to ensure the efficient operation and that all the resources are utilised optimally;

Participate in the development and implementation of Architectural mechanisms for Solution Security;

Security Development to improve security of government systems;

Programmes/projects manage development/procurement and maintenance projects of Solution Security so as to meet Solution Security: Security Development service delivery commitments;

Ensure that all SITA and Government infrastructure has the correct level of protection to ensure secure operation, by managing, achieving and maintaining appropriate protection level of data and systems;

Develop and execute stakeholder relationship management plans to enable effective management and improvement of stakeholder relationships; and

Ensure that resources are kept abreast of the latest industry developments and ensure that appropriate technologies are used for knowledge management so as to ensure that innovation and improved productivity;

Qualifications and Experience

Minimum: Diploma/Bachelors degree in an ICT related field (Computer Science, Information Systems, Technology and Engineering) or equivalent.

Experience: 8 - 9 years' experience in the ICT security architecture environment with leadership, general management, operational responsibility in a large corporate/public sector organisation. The experience must include:

- Experience as a Senior Manager in corporate/public sector; and
- Experience in ICT security architecture environment within the corporate/public sector, including:

  - Strategic thinking and leadership with strong abilities in relationship management;
  - Established a track record of managing technical staff (Cross-functional environment experience highly desirable);
  - Data administration and security methods;
  - Multiplatform platform environments and their operational/security considerations;
  - Demonstrated project management competency and the execution of multiple projects, including managing resources across multiple projects; and
  - Developed efficient and effective IT security solutions to diverse and complex business problems.

Technical Competencies Description

Knowledge of: ICT Charter and ICT Business Environment and Landscape; SITA ICT Solutions (Information Security); Government's Technical Operations; Implementation Capability Models; Project Management; Solution Delivery Lifecycle; Enterprise Architecture Framework; Governance Processes and Standards; Analysis and Design Methods; Architectures; Information System Security Technical Standards; Security Standards and Frameworks; Solution Development Lifecycle; Infrastructure Security and Data Security; Enterprise architecture framework (TOGAF; Zachman; FEAF; MODAF; GWEA Framework; MIOS); Governance Processes and Standards (ISO 9001; ISO 27001/ 27002; ISO 12207 (SDLC); ISO 42010; COBIT; ITIL; UML); Project Management principles (PM Bok/ Prince 2); Broad knowledge of 7/10 CISSP domains (CISSP,CISA,CISS,CCSA,CSCE); CISM (Certified information security Manager) or CISA (Certified information systems Auditor); Analysis and Design Methods (SSADM / OOADM); Service Oriented Architecture (SOA); Information System Security Technical Standards (PKI, IAM, Cryptography).

Skills: Capacity Planning and Resource Management; Strategy and Policy Formulation; Budget and Finance Management; Risk Management; Asset Management; Stakeholder Management; People management; Auditing & Analytical; Monitoring and Reporting; Planning & Organising; Fraud Awareness; Stakeholder Management; Customer Relationship Management; Initiative and Innovation; Customer Service; People Management; Negotiations; and Communication.

Other Special Requirements

The incumbent will be required to engage with various stakeholders/role players such as SSA (State Security Agency), NIA, SAPO and external parties to deal with State Security related issues, inclusive of assisting with international and national investigations.

How to apply

Kindly send your CV to rachel.recruitment@sita.co.za

Closing Date: 18 October 2018

Disclaimer

SITA is an Employment Equity employer and this position will be filled based on Employment Equity Plan. Correspondence will be limited to short listed candidates only. Preference will be given to members of designated groups.

- If you do not hear from us within two months of the closing date, please regard your application as unsuccessful.
- Applications received after the closing date will not be considered. Please clearly indicate the reference number of the position you are applying for.
- It is the applicant`s responsibility to have foreign qualifications evaluated by the South African Qualifications Authority (SAQA).
- Only candidates who meet the requirements should apply.
- SITA reserves a right not to make an appointment.
- Appointment is subject to getting a positive security clearance, the signing of a balance score card contract, verification of the applicants documents (Qualifications), and reference checking.
- Correspondence will be entered to with shortlisted candidates only.
- CV`s from Recruitment Agencies will not be considered.